Annual ADFSL Conference on Digital Forensics, Security and Law 2014

May 29th, 1:00 PM

Application Of Toral Automorphisms to Preserve Confidentiality Principle in Video Live Streaming

Enrique García-Carbajal
National Polytechnic Institute of Mexico, egarciac1206@alumno.ipn.mx

Clara Cruz-Ramos
National Polytechnic Institute of Mexico, ccruzra@ipn.mx

Mariko Nakano-Miyatake
National Polytechnic Institute of Mexico

APPLICATION OF TORAL AUTOMORPHISMS TO PRESERVE CONFIDENTIALITY PRINCIPLE IN VIDEO LIVE STREAMING

Enrique García-Carbajal
egarciac1206@alumno.ipn.mx

Clara Cruz-Ramos
ccruzra@ipn.mx

Mariko Nakano-Miyatake
Mechanical and Electrical Engineering School
Graduate Section ESIME Culhuacan
National Polytechnic Institute of Mexico
Av. Santa Ana 1000 Col. San Francisco Culhuacan
04430, México City. México

ABSTRACT

Most of the Live Video Systems do not preserve the Confidentiality principle, and send all frames of the video without any protection, allowing an easy "man in the middle" attack. But when it does, it uses cryptographic techniques over streaming data or makes use of secure channel systems. This generates low frame rate and demands many processor resources. In fact native Live Video Streaming demands many resources of all System.
In this paper we propose a technique to preserve confidentiality in Video Live Streaming applying a confusing visual method making use of the Toral Automorphism Spatial Transformation over each frame. In terms of agreeing robustness to this algorithm, we agree on two criteria: (1) Before reallocating subframes, rotate some of them 180°; and (2) Randomly choose a key to change the order of reallocating subframes.

Keywords: toral automorphism, spatial transformation, subframe, man in the middle, iterations.

1. INTRODUCTION

The Information Security is a set of preventive and reactive measures of organizations and technologic systems to safeguard and secure the information; trying to maintain the integrity, availability and confidentiality of it.

1.1 Integrity, Availability and Confidentiality

Integrity is intended to guarantee that a message or file is not modified without authorization from its creation or during its transmit across an informatics network. By this way, it is possible to detect if any data has been added or deleted.

An Availability service is important to guarantee the objectives. The system must be robust enough to face attacks and interferences, securing its correct operation.

As part of the Availability service we can consider the recovering of the system when it has been successfully attacked or damaged by natural disasters.

The Confidentiality function implies that every single message transmitted or stored can be read only by its genuine receiver. If a message is intercepted by another hand, they could not get the original

message. So this service pretends to secure confidentiality of storage data and/or transmitted data across communication networks.

1.2 Approach

Because of the characteristics of live video, we do not focus on the Integrity principle too much; for example, when a frame is lost. We do not need to request a retransmission of the frame unless it is needed by the system because it can be replaced in time by the next frame.

Few times the Availability principle can be covered just with an algorithm, so our approach is mainly oriented to the Confidentiality principle.

2. TORAL AUTOMORPHISM

A two-dimensional "torus automorphism" can be considerate as a spatial transformation of planar regions which belong to a square two-dimensional area. A great subset of one-parameter family of two-dimensional toral automorphism is defined as follows:

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ k & k+1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} (mod\ N) \qquad (1)$$

where $(x_n, y_n) \in [0, N-1]\mathrm{X}[0, N-1]$

All the orbits of the system (1) are unstable periodic orbits with periods *T*, which depend on *k*, *N* and the beginning point of the orbit [5].

Evaluating for $\begin{pmatrix} x_{n+2} \\ y_{n+2} \end{pmatrix}$

$$\begin{pmatrix} x_{n+2} \\ y_{n+2} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ k & k+1 \end{pmatrix} \begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} (mod\ N) \qquad (2)$$

Replacing $\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix}$ from (1) to (2):

$$\begin{pmatrix} x_{n+2} \\ y_{n+2} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ k & k+1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ k & k+1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} (mod\ N) \qquad (3)$$

thus,

$$\begin{pmatrix} x_{n+2} \\ y_{n+2} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ k & k+1 \end{pmatrix}^2 \begin{pmatrix} x_n \\ y_n \end{pmatrix} (mod\ N) \qquad (4)$$

In general terms, if we have an initial coordinate $(x_0, y_0) \in [0, N-1]\mathrm{X}[0, N-1]$ it could be demonstrated that

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ k & k+1 \end{pmatrix}^n \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} (mod\ N) \qquad (5)$$

with $(x_n, y_n) \in [0, N-1]\mathrm{X}[0, N-1]$.

So, *n* can be seen as the number of iterations made over (x_0, y_0)[1].

3. DEVELOPMENT

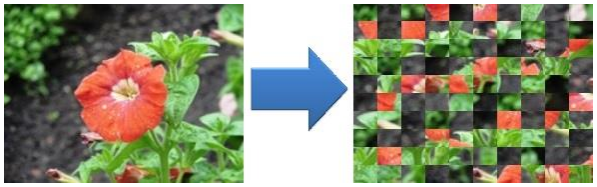
Using the toral automorphism equation (5) as a vector generator over each pixel of a two-dimensional square digital image I_0, we can obtain a new image I_n with the same dimensions as I_0 in which each pixel is reallocated in a new position given by (5), and the order of allocation depends on three integer variables: *k*, *n* and *N*.

(a) (b) (c)

Figure 1 Toral automorphism Applied to a Lena Image, with Different Iterations. a) Image of "Lena", b) Mixing of "Lena" with n=1, b) Mixing of "Lena" with n=5.

3.1 Choosing parameters

The basic principle of video is the fast display of images in sequence called "frames". We can apply the method mentioned above to each video frame by creating a kind of visual cryptography; however, an inconvenient is the high demand of processing needed to reallocate each pixel into its new position. The proposed algorithm uses sub-frames instead of pixels [3]. Dividing each frame in *N* X *N* subframes, this algorithm reallocates each subframe in a new position in frame and it can be easily processed by a Graphics Processing Unit (GPU) [2], instead of a cryptographic method when main processing is given by the Central Processing Unit (CPU). Before being processed by toral automorphism, the frame with dimensions *HxW* is divided in subframes with dimensions (*H/N)x*(*W/N)*. So, for example, the upper left subframe before processing will have assigned the coordinate *(0, 0)* and the lower right subframe, the coordinate *(N-1,N-1)*.



(a) (b)

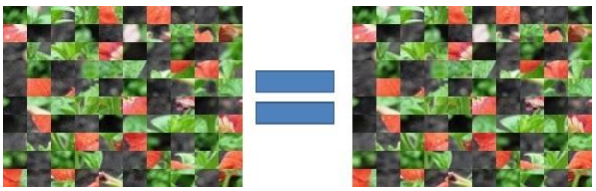
Figure 2 Frame Processing with the Proposed Sub-Frames Toral Automorphism Algorithm. (a) Original Frame with HxW Dimensions, (b) Original Frame Divided and Processed with 10x10 Subframes, N=10, n=2, and k=5.

We can obtain different order of coordinates for the same *NxN* subframes, changing *k* and *n*, because *k* gives the angle of generated vectors and *n* reallocate *n* times the subframes.

(a) (b)

Figure 3 Processed Frame with Same N, but Different n and k. (a) Processed Frame with n=2 and k=14, (b) with n=4 and k=23.

It is important to say that due to the cyclic and modular properties of this automorphism, we can obtain the same coordinates in a *NXN* divided frame for different *k* and *n.*



(a) (b)

Figure 4 Same Subframes Distribution with Different n and k. (a) Processed Frame with n=2 and k=4, (b) with n=2 and k=14.

One of the purposes of the algorithm is to create visual confusing to preserve confidentiality. Then the choice of *k* and *n* is very important. A Wrong choice of this pair can result in ineffectiveness for such purpose as seen in fig 5.

(a) (b)

Figure 5 Comparison of Original and Processed Frames with Bad Choice of k and n. (a) Original Frame, (b) Processed Frame with Bad Choice of k and n.

A "man in the middle" attack has more probability of success if our pair *k* and *n* are wrongly chosen because the original frame could be easily recovered.

There is also an important consideration and it is the direct relation between *N* and the time of processing. It means that, if we increase the number of subframes *N*X*N*, it takes more processing time to GPU to reallocate sub-frames than with a minor value of *N*.

3.2 Streaming

There are many ways to send a frame by a channel, and it depends on the system requirements. However, streaming a live video is a bit different to sending a stored video. Sending a stored video implies that we do not see that video in real-time. So we can agree an error correction or detection code to the system and preserve the integrity principle for it. It is almost impossible to implement in live video, because if a frame is received with errors, it is quickly replaced with the next frame.

UDP and RTCP protocols are very used in streaming live video over IP, instead of TCP that sends a transmission request if a frame is received with errors.

3.3 Steganography

Steganography is the art and science of hiding communication; a steganographic system thus embeds hidden content in unremarkable cover media so as not to arouse an eavesdropper's suspicion. In the past, people used hidden tattoos or invisible ink to convey steganographic content. Today, computer and network technologies provide easy-to-use communication channels for steganography [4].

Talking about digital systems, it differs from cryptography because with cypher methods somebody knows that a message is here but they could not recover a message unless they have the proper keys. In steganography, the sender hides a message and the receiver knows it is there but everyone else does not.

3.4 Proposal

A "man in the middle" hacker can have the patience for manually reallocating the sub-frames like a puzzle game, and one of the proposed strengthening is to spin 180° some selected sub-frames, for example odd sub-frames; before reallocate it with toral automorphism process. The second proposal is the pseudorandom changing of k each specific time. This means that we are working with a set of different k (called k_i) and it will change the order of the reallocated subframes. After a frame has been processed, we must insert with a steganographic technique a k_i id, that the receiver can understand. Both sender and receiver must have the same previous knowledge of k_i, N, n, W and H values.

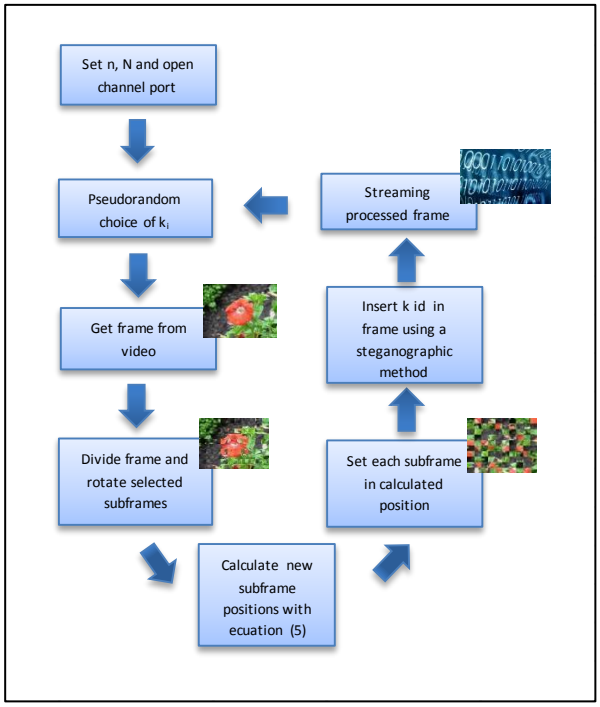


Figure 6 Sender Schema

To recover a frame as original on the receiver side it is necessary to follow similar steps as the sender, with minor changes.

First, it is necessary to recover k, extracting it by the inverse steganographic method. The next step is to reverse the toral automorphism process.

It can be demonstrated that the inverse process for toral automorphism is given by

$$\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} k+1 & -1 \\ -k & 1 \end{pmatrix}^n \begin{pmatrix} x_n \\ y_n \end{pmatrix} mod(N) \qquad (6)$$

Hence, the equation (6) must be used in the receiver side after recovering the key id, in order to calculate and return each subframe to the original position.

The following step is to rotate back the selected subframes. Both, sender and receiver previously was agreed which of them will be overturned.

Finally, the receiver gets a frame that can be displayed or stored with the confidentiality principle preserved and without the help of cryptography methods or secure channels.

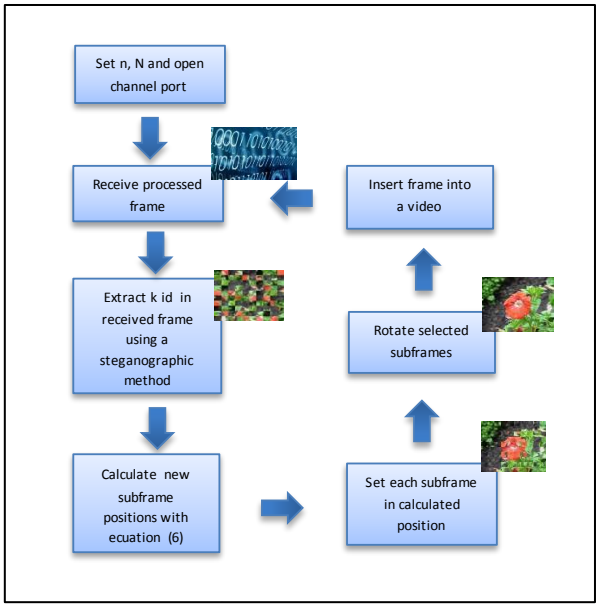


Figure 7 Receiver Schema

4. CONCLUSIONS

The proposal method needs math computing to calculate the coordinates of subframes to be reallocated. However it can be calculated in the beginning of the process, generating a set of coordinates-arrays for a given keys k_i and n; then the GPU can just ask for the calculated coordinates and so reallocate the subframes.

For system designing, there are lot of powerful ready-to-use CPU, GPU and Single Board Computers in market. It is also important the protocol and channel chosen to have an optimal communication between the sender and receiver systems, and it can be combined with cryptographic systems and algorithms. The best choice will be given through a cost-requirements study.

There are some libraries for CPU/GPU that allow an easy image processing, like its conversion to string and vice versa, DCT transformation, wavelet transformations, cut and paste sections, rotating, drawing geometric forms, filters, etc. It could be an easy tool for processing frames and inserting the parameters needed into the processed frame and recover a frame as original.

If a visible watermark is needed, like a copyright authentication, it is recommended that the receiver does that job. A visible watermark can be useful for a "man in the middle" hacker to reconstruct an intercepted frame because some parts of the watermark will be in spaced in different frames.

5. ACKNOWLEDGMENTS

We thank Instituto Politécnico Nacional de México (National Polytechnic Institute of Mexico), COFAA and the National Council for Science and Technology (CONACyT) of Mexico for the support provided during the course of this research. Also, we thank the reviewer for the useful suggestions to improve the paper.

REFERENCES

Arora, M., Nath, S., Mazumdar, S., Baden, S.B., & Tullsen, D.M. (2012). Redefining the Role of the CPU in the EEra of CPU-GPU Integration. *Micro, IEEE*, *32*(6), Nov.-Dec, 2012, 4, 16.

Zhang, Nan, Chen, Yun-shan, Wang, & Jian-Li. (2010). Image parallel processing based on GPU. 2010 2nd International Conference on Advanced Computer Control (ICACC), 3, 27-29 March 2010, 367 and 370.

Petersohn, C. (2007). Sub-Shots-Basic units of video. Systems, Signals and Image Processing, 2007 and 6th EURASIP Conference focused on Speech and Image Processing, Multimedia Communications and Services. 14th International Workshop, 27-30 June 2007, 323 and 326.

Provos, N., & Honeyman, P. (2003). Hide and seek: An introduction to steganography. *Security & Privacy, IEEE, 1*(3), May-June 2003, 32 and 44.

Voyatzis, G., & Pitas, I. (1996). Applications of toral automorphisms in image watermarking. Image Processing, 1996. Proceedings, International Conference, 1, 16-19 Sep 1996, 237 and 240.